FOUNDATION FOR AMERICAN INNOVATION

June 13, 2023

Geoffrey Cain
Senior Fellow, Foundation for American Innovation
Written Testimony for U.S. Senate Committee on the Judiciary
Subcommittee on Human Rights and the Law

"America, the Vanguard of Democracy, Must Stand Up to China's AI Totalitarianism"

Chairman Ossoff, Ranking Member Blackburn, and members of the Subcommittee:

Thank you for the opportunity to testify today. My testimony has two purposes:

1. First, to outline how China has created the world's most sophisticated and terrifying surveillance state using novel artificial intelligence (AI) technologies, and how American business elites helped make this happen.

2. Second, to suggest ways that the US can defend the use of AI with respect to democracy and human rights, to ensure that the Chinese Communist Party (CCP) cannot advance its malign global agenda with AI tools.

With AI, America's elites have learned little about the perils of engaging with China's one-party authoritarian state

On Friday, OpenAI CEO Sam Altman dialed into the annual conference at the Beijing Academy of Artificial Intelligence, three weeks after he testified before another subcommittee here at the Senate Judiciary Committee. He called on the People's Republic of China—a one-party authoritarian state that has used AI to carry out genocide against an ethnic minority—to help shape global AI safety guardrails. "With the emergence of increasingly powerful AI systems," he said, "the stakes for global cooperation have never been higher."[1]

To anyone who's lived in China, this was a curious and mind-boggling call to action. The Chinese Communist Party (CCP) has engineered a vast AI-powered surveillance system literally called "Sky Net." It runs AI-powered "alarms" that notify the police and intelligence services when someone unfurls a banner,[2] when a foreign journalist is traveling to certain parts of the country,[3] and when someone from an ethnic minority is

[1] Sarah Zheng, "OpenAI's CEO Calls on China to Help Shape AI Safety Guidelines," Bloomberg Technology, June 9, 2023, https://www.bloomberg.com/news/articles/2023-06-10/openai-s-ceo-altman-calls-on-china-to-help-shape-ai-safety-guidelines.

[2] Gulchehra Hoja, "In China, AI Cameras alert police when a banner is unfurled," *Radio Free Asia*, June 5, 2023, https://www.rfa.org/english/news/china/surveillance-06052023142155.html.

[3] Jimmy Quinn, "'Total Security State': Shanghai Intensifies Surveillance of Foreign Journalists Who Go to Xinjiang," *National Review*, May 2, 2023, https://www.nationalreview.com/corner/total-security-state-shanghai-intensifies-surveillance-of-foreign-journalists-who-go-to-xinjiang/.

present.[4] The government accuses entire groups, such as Muslim Uyghurs, of posing a terrorist threat, and relentlessly persecutes them with the use of AI tools.

It sounds like a dystopian science fiction story—think *1984* or *Minority Report*—but the CCP's AI totalitarianism has become a fact of daily life for the more than 1.4 billion people in China. In fact, the Chinese technologists who spoke at the same conference as Mr. Altman were some of the very people who built this monstrosity. They were executives at iFlyTek and Huawei, two AI giants and are heavily sanctioned by the US government for their involvement in human rights abuses.[5] If Mr. Altman plans on cooperating with China's AI developers, he better figure out who he's working with.

I've witnessed the results of their work firsthand. As an investigative journalist formerly in China, I was among the first people to document and expose the horrific surveillance state that oppressed the Uyghur population in the far western region of Xinjiang. Since 2017, the atrocity has morphed into the largest internment of ethnic minorities since the Holocaust, which the US State Department calls a genocide.[6]

Chinese authorities have hauled away 1.8 million people to concentration camps—about one-tenth of the ethnic minority population in Xinjiang—and have forced many of them into slave labor.[7] Because they have read too many books or have been caught praying, they have been declared enemies of the state, despite not being formally charged with any crime. This was all with the help of the AI surveillance system that scooped up data from facial recognition, voice recognition, and a network of police cameras covering every possible square inch of the region. Party authorities told Uyghurs they wanted to "cleanse" their minds of what they called "ideological viruses."

In December 2017, I was kicked out of China while researching my book, *The Perfect Police State: An Undercover Odyssey into China's Terrifying Surveillance Dystopia of the Future.* Ever since then, the AI-fueled police state has expanded to alarming levels. In 2018, I moved to Turkey and, for three years, tracked down former intelligence officers from China's Ministry of State Security, the powerful and secretive intelligence body. They had helped set up the AI surveillance systems in Xinjiang, were targeted by those same systems because they were Uyghurs, and then defected to safety.

[4] Drew Harwell and Eva Dou, "Huawei tested AI software that could recognize Uighur minorities and alert police, report says," *Washington Post*, December 8, 2020, https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/.

[5] Karen Hao, "Open AI CEO Calls for Collaboration with China to Counter AI Risks," *The Wall Street Journal*, June 10, 2023, https://www.wsj.com/articles/openai-ceo-calls-for-collaboration-with-china-to-counter-ai-risks-eda903fe.

[6] Secretary of State Michael R. Pompeo, "Determination of the Secretary of State on Atrocities in Xinjiang," U.S. Department of State, January 19, 2021, https://2017-2021.state.gov/determination-of-the-secretary-of-state-on-atrocities-in-xinjiang/index.html.

[7] Adrian Zenz, "China's Own Documents Show Potentially Genocidal Sterilization Plans in Xinjiang," *Foreign Policy*, July 1, 2020, https://www.wsj.com/articles/openai-ceo-calls-for-collaboration-with-china-to-counter-ai-risks-eda903fe.

These intelligence officers drew detailed diagrams in my possession that showed the workings of these surveillance systems and how facial recognition and voice recognition technologies helped fuel them. What they revealed was alarming, but not surprising. The highest echelons of CCP leadership held centralized control over many AI surveillance systems, as well as direct lines of influence over Chinese mega-companies such as Huawei and ByteDance. With the help of these companies, China's government had been making a concerted, malicious effort to expand these surveillance capabilities all over the world.

The development of AI is at the heart of China's global ambitions

The surveillance state that began in Xinjiang was a taste of the horrific power of AI when placed in the wrong hands. "Advanced technology is the sharp weapon of the modern state," China's President Xi Jinping said in a 2013 speech.[8] In July 2017, China unveiled its National AI Development Plan, calling AI a "historic opportunity" and pledging to align developments in AI with the government's authoritarian values. China has declared its goal as becoming the world leader in AI by 2030.[9] The goal reflects the totalitarian ambitions of President Xi, who has led the efforts to clamp down Uyghurs, Tibetans, Mongolians, and religious and political dissidents of all stripes.

Since then, we've seen the expansion of China's technology companies, using AI and other novel developments, all over the world. Huawei, the heavily sanctioned telecommunications firm, has led efforts to establish global surveillance systems, usually under the guise of AI-powered "smart cities" designed to fight crime and regulate traffic, but that in reality have been used to equip governments with the tools to spy on political dissidents. In October 2022, the FBI arrested two Chinese nationals who stood accused of bribing an undercover FBI officer to obtain inside intelligence about an investigation into Huawei.[10]

Meanwhile, ByteDance, the $220 billion mega-firm that owns TikTok, stands accused by a whistleblower of running an in-house CCP Committee that had access to all the app's data, including data stored in the US, according to a court filing.[11] Other sanctioned, lesser-known firms, such as AI facial and voice recognition companies iFlyTek, SenseTime, and Megvii, have emerged as global billion-dollar unicorns with the backing of the Chinese state and the involvement of US venture capital funds.

[8] Chris Buckley and Paul Mozur, "What Keeps Xi Jinping Awake at Night," *New York Times*, May 11, 2018, https://www.nytimes.com/2018/05/11/world/asia/xi-jinping-china-national-security.html.

[9] Graham Webster, Roger Creemers, Elsa Kania, and Paul Triolo, "Full Translation: China's 'New Generation Artificial Intelligence Plan,'" August 1, 2017, https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

[10] Glenn Thrush and David McCabe, "Justice Dept. Charges 2 Chinese Citizens With Spying for Huawei," *New York Times*, October 24, 2022, https://www.nytimes.com/2022/10/24/us/politics/justice-dept-huawei.html.

[11] Thomas Fuller and Sapna Maheshwari, "Ex-ByteDance Executive Accuses Company of 'Lawlessness,'" *New York Times*, May 12, 2023, https://www.nytimes.com/2023/05/12/technology/tiktok-bytedance-lawsuit-china.html.

This situation is proving hard to continue in the age of technological decoupling. This month, Sequoia Capital, the preeminent venture capital firm that originally invested in Apple and Facebook, announced that it was splitting off its Chinese arm into a separate company.[12] Sequoia's China business was core to helping build China's AI industry, with a reported $22 billion stake in ByteDance, to name one of many examples.[13] Sequoia's spin-off suggests that American business executives are waking up to the unavoidable risks of doing business in China—of inadvertently helping build China's AI systems that damage human rights and the public good.

Generative AI is a threat to CCP censorship

In April 2023, the Cyberspace Administration of China announced draft regulations for generative AI, setting down potential rules that chatbot-produced content follow "socialist core values" and avoid information that undermines "state unity."[14] The CCP's goal is a continuation of its past strategy to align new technologies and censor information in line with its political values. ChatGPT has not made its service available in China, but there is already significant demand. The black market is already flourishing with offerings of overseas ChatGPT access to people in China, but these days could be numbered.[15]

Generative AI, however, is a departure from the surveillance technologies that have defined the evolution of China's political censorship. Generative AI services have the potential to empower regular people who want to produce large amounts of content that challenge government propaganda and narratives. The question is whether China's "Great Firewall"—the harsh internet censorship system—can stand up to the potential of generative AI. Will China one day see an information renaissance, with stories of the Tiananmen Square massacre and Hong Kong protestors spread across the internet through uncontrollable chatbots?

Given the CCP's enormous success at censorship so far, I believe that it will once again succeed in coercing and coopting Chinese technology firms and transforming generative AI into a tool of state oppression. American technologists will unwittingly assist CCP goals if they cooperate too eagerly with state-connected Chinese companies, institutes, and people. As we have learned over the last decade, this is the sad truth of being a technologist in China.

[12] Shawn Johnson, "Neil Shen goes it alone in China after Sequoia split," *Financial Times*, June 9, 2023, https://www.ft.com/content/179eb51a-70eb-4c79-9e74-befd0f5a02b7.

[13] Alex Kondrad, "For Top VCs, ByteDance's Historic Windfall Remains a $220 Billion Mirage," *Forbes*, May 4, 2023, https://www.forbes.com/sites/alexkonrad/2023/05/04/bytedance-scrutiny-leaves-midas-investors-waiting-billions/.

[14] Chang Che, "China Says Chatbots Must Toe the Party Line," *New York Times*, April 24, 2023, https://www.nytimes.com/2023/04/24/world/asia/china-chatbots-ai.html.

[15] Caiwei Chen, "China's ChatGPT Black Market Is Thriving," *Wired*, March 7, 2023, https://www.wired.com/story/chinas-chatgpt-black-market-baidu/.

The US must use its global technological leadership to protect democracy and human rights from China's AI threats

The CCP is the greatest threat to human rights and democracy around the world. Although China is quickly catching up to US innovation, the US remains the leader in AI development. We must abandon the misguided idealism of working with Chinese companies and government bodies with the hope that AI will change the political system, allow for the opening of democratic discourse, and create safer global AI regulations. Rather than helping advance innovation, we will be doing the world a disservice by handing the keys to the CCP. Under Chinese law, these advanced AI applications will inevitably be used to oppress human rights and expand China's authoritarian footprint.

Rather, we should use our position of strength and our democratic values to carry out a two-fold strategy. First, AI talent and innovation must flow towards the direction of America and its allies. We must influence global AI standards, attract global AI talent away from China, and secure our software and hardware ecosystems from China's malign influences. Second, the most advanced American technologies and investments must not be allowed to flow in the direction of China. We must work against China's ambitions to develop advanced AI systems, influence global standards, and oppress dissidents around the world. The specific policy steps are as follows:

1. **The US must take the lead in developing global AI standards that uphold human rights and democratic values.**

   The CCP has loudly used multilateral membership bodies—the United Nations, the World Health Organization, and so forth—to shape global technology and science standards in its interests and to make countries all over the world dependent on Chinese technological innovation. The US must not shirk its global leadership, which would mean ceding ground to China and abandoning our allies in a moment of global struggle.

   In November 2021, 193 countries adopted the first-ever global agreement of AI ethics under the United Nations Educational, Scientific, and Cultural Organization (UNESCO), calling for a "do no harm" principle, personal data protection, and measures to prevent fairness and non-discrimination.[16] The US should leverage other United Nations bodies and the International Organization for Standardization (ISO) to build democratic AI principles and ensure that China's authoritarian goals do not crush the principles of human rights.

2. **American companies that help build China's oppressive AI ecosystem must be held accountable.**

[16] UNESCO, "Recommendations on the ethics of artificial intelligence," November 2021, https://www.unesco.org/en/articles/unesco-adopts-first-global-standard-ethics-artificial-intelligence.

China built its AI surveillance apparatus with the connivance and complacency of major American technology firms. The science corporation Thermo Fisher, for example, was caught selling DNA collection equipment directly to Xinjiang police authorities who used them for mass gathering of genetic data on the minority Uyghur population.[17] Since the late 1990s, Microsoft has established itself as the training ground for China's AI elites through its Beijing-based laboratory, Microsoft Research Asia. The laboratory has trained many of the AI leaders and developers who went on to found or join the executive leadership of rights-abusing firms such as Sensetime, Megvii, and iFlyTek. Beginning in 2019, the US government has sanctioned these individuals and their companies.[18]

So far, American technology giants have faced no punishment for their involvement in China's surveillance state. This subcommittee may consider drafting a bill that requires public corporations to publish their due diligence reports on their activities in China and the risks they have encountered with regards to human rights there. The subcommittee may also consider drafting a bill that criminalizes specific American business activities in China that are likely to support, directly or indirectly, human rights abuses by the CCP. This would include prison time for American business executives involved helping develop any form of AI in partnership with a Chinese entity, if the CCP will likely use that technology for the oppression of human rights and democratic values.

3. **Because Chinese software companies are required to partake in Chinese state intelligence operations, they should be compelled to separate their American businesses.**

Over the past decade, China has enacted a raft of draconian laws, such as the National Security Law and the National Intelligence Law, that require people in China to assist the government in intelligence-gathering when called upon, among other requirements.[19] While we in America have a system of due process and checks and balances that can guard against data overreach, in China no such rights exist. The private and personal data of Americans is not safe in the hands of Chinese-owned apps such as TikTok and Temu, whose owners and employees in China are required to hand over data to the state if it's requested.

Apps like TikTok are beginning to form the core of the US information environment, with sophisticated algorithms that recommend highly addictive

[17] Human Rights Watch, "China: Minority Region Collects DNA from Millions," December 13, 2017, https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions.
[18] Kate Kaye, "Microsoft helped build AI in China. Chinese AI helped build Microsoft," *Protocol*, November 2, 2022, https://www.protocol.com/enterprise/us-china-ai-microsoft-research.
[19] Bonnie Girard, "The Real Danger of China's National Intelligence Law," February 23, 2019, https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/.

content, while being used to spy on US citizens.[20] This is a gaping breach of our ability to protect democratic values and human rights here in the US. In the event of conflict with China—an increasing likelihood with China's aggressive military posture—these apps have the potential to become misinformation machines designed to manipulate Americans with sophisticated and algorithmic propaganda. The solution is to force these firms to spin off their American operations into separate companies, ensuring their safety from CPP meddling.

4. **America and its allies must secure and coordinate global supply chains for advanced AI logic chips.**

   The US has made remarkable progress in legislating and implementing export controls that prevent American firms from selling advanced chips and their components to China. In October 2022, the Biden administration implemented the most recent round of sanctions, restricting the export of certain services and equipment to China, effectively placing China generations behind American chip technologies for the latest AI applications.[21] Four months later, in February 2023, the Department of Commerce opened the first round of company grants under the CHIPS and Science Act, hoping to reshore semiconductor manufacturing capabilities and make the US more self-sufficient.[22]

   The CHIPS and Science Act, however, is the starting point and not the last step. Advanced semiconductors are the most complex devices that humankind has ever made—and they cannot simply be manufactured end-to-end in the US. Chip supply chains depend on thousands of suppliers all over the world. The US needs to better coordinate with its key chip-producing and component-producing partners—South Korea, Taiwan, Japan, and the Netherlands—by upgrading the "Chip 4" talks into a formal consortium for coordinating R&D innovations.

   The upgrade will enhance the implementation of the CHIPS and Science Act and the future of AI technologies by adding an element of multilateralism. Our technological partners will have better reason to believe their contributions to the US manufacturing ecosystem are profitable and worthwhile, a hedge against CCP aggression. If we can form a true semiconductor alliance, China will be unable to bully individual countries into supplying critical chip technologies for its AI systems.

[20] Emily Baker-White, "TikTok Spied on Forbes Journalists," *Forbes*, December 2, 2022, https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=3b7173b97da5.

[21] Demetri Sevastopulo and Kathrin Hille, "US hits China with sweeping tech export controls," *Financial Times*, October 7, 2022, https://www.ft.com/content/6825bee4-52a7-4c86-b1aa-31c100708c3e.

[22] U.S. Department of Commerce, "Biden-Harris Administration Launches First CHIPS for America Funding Opportunity," February 28, 2023, https://www.commerce.gov/news/press-releases/2023/02/biden-harris-administration-launches-first-chips-america-funding.

As we enter the unprecedented age of generative AI, we must not allow China, a one-party authoritarian state, to infect the global AI ecosystem where it will oppress human dignity, civil liberties, and rule of law. We have seen the CCP's willingness to carry out genocide against its people with the help of AI surveillance systems. Now we must find ways to ensure that the words "never again" hold true. Thank you, Senators, for having me here today. I look forward to answering your questions.